

Arkansas Health Information Exchange
Legal and Policy Strategic Plan – Draft 3-14-10

Describe the state's privacy and security framework, which must consider federal and state laws and regulations and adherence to the privacy principles articulated in the HHS Privacy and Security Framework.

1. Privacy and Security Framework

HHS has identified eight privacy principles

http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf which the Arkansas Health Information Exchange will follow. These principles will be addressed as follows:

- Individual Access
- Correction
- Openness and Transparency
- Individual Choice
- Collection, Use and Disclosure Limitation
- Data Quality and Integrity
- Safeguards
- Accountability

Provide plans to analyze and/or modify state laws.

2. State Laws

Describe plans to develop policies and procedures necessary to enable and foster information exchange within the state and interstate.

3. Policies and Procedures

Describe plans to communication and/or negotiate with other states to enable exchange.

4. Exchange Between States

Describe existing trust agreements that enable the secure flow of information among parties.

5. Trust Agreements

Describe stakeholder endorsement of the statewide policy framework.

6. Stakeholder Endorsement and Oversight

Legal/Policy

The Privacy and Security Officer of the Office of HIE will be assigned primary responsibility for ensuring that the HIE system operates in compliance with all current and future state and Federal laws, statutes, regulations and rules related to privacy and security of health information. The HIE policies and procedure will be drafted in accordance with the privacy principles articulated in the US Department of Health and Human Services (USDHHS) Privacy and Security Framework. The Principles, as articulated by ONC, form a core framework upon which all policies are developed.

Privacy and Security

The Privacy and Security Office will build upon analyses conducted in the Arkansas Health Information, Privacy and Security Collaboration (HISPC) and the Robert Wood Johnson Arkansas Regional Quality Improvement (RQI) projects that form the core of the State's health information / health information technology plan. These initiatives addressed use cases, barriers and solutions for addressing inter and intrastate HIE.

Through these projects a number of state and Federal laws that impact health information were identified. These include but are not limited to the following laws regarding consent, authorization and release of information:

The ONC HIT principles form a core framework upon which all policies are developed. These principles guarantee exchange participants the following rights and assurances: a) Individual access to a person's own PHI, b) Ability to correct misinformation in the electronic, c) Openness and transparency of the operation of the Initiative, d) Individual input as regards use of their information, e) Limitations on use and disclosure of an individual's PHI, f) Integrity of the data, g) Security of the data and h) accountability by those violating data protocols.

State and Federal Laws

The RQI and HISPC projects identified and collected all applicable state and Federal laws pertinent to privacy and security of electronically exchanged health information including those as detailed supra. The Privacy and Security Office will monitor legal databases, the Federal Register and other sources to ensure awareness and compliance with all applicable authority as well as current and to be developed standards for health information exchange promulgated by the Office of the National Coordinator for Health Information Technology. The Strategic Plan will address existing laws regarding health information privacy and security:

State of Arkansas

ACA 20-9-602 – Persons other than then patient who may consent, authorize, or allow release of information

ACA 20-9-603 – Consent, authorization and release of information in emergent situations.

ACA 9-25-101 – Release of patient information to law enforcement personnel

ACA 20-15-904 – Confidentiality of HIV/AIDS data and information

Additionally, the Strategic Plan will identify state laws in the following areas to determine application to the exchange;

- Health care provider / institution licensing and regulation statutes.
- State laws incorporating the Federal Uniform Electronic Transactions Act
- Statutes controlling use of social security numbers

- Arkansas HIPAA statutes, rules and regulations

Federal

45 CFR 164.502(a)(11)(ii) – Consent to treat and / or release information in emergent situations.

42 CFR 2.12(c)(e)(b) – Statute limitations on emergency room personnel

45 CFR Part 160 - Health Information Portability and Accountability Act Privacy Standards

45 CFR Part 164 – Health Information Portability and Accountability Act Security Standards

Policies and Procedures

The Privacy and Security Office will oversee drafting of policies and procedures that comply and comport with appropriate authorities as well as the privacy principles articulated in the HHS Privacy and Security Framework.

Trust Agreements

The HIE System will oversee development and implementation of trust agreements between state agencies that will allow for the secure electronic exchange of health information and data between and among participants in the HIE System. These contractual and cooperative agreements include but are not limited to; data use agreements, data sharing agreements, business agreements, and reciprocal support agreements. All such agreements will reference appropriate state and Federal authority and will include both legal and contractual penalties for non compliance, non performance and improper access to / release of data and information.

Oversight of Information Exchange and Enforcement

The Privacy and Security Officer will have primary responsibility for ensuring that data in the exchange is maintained in a safe and secure manner. The Officer shall develop and implement a series of data access and compliance audits, and reports any non compliance to the appropriate authority. Privacy and Security Office staff will assist state and Federal authorities in investigation and / or prosecution of unauthorized data access and / or release.